

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-PC-2025 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

中标华信（北京）认证中心有限公司认证规则公开方式或可获取的途径：本中心认证规则信息依法依申请公开，如需获取经备案的认证项目认证规则全文请发函至本中心**邮箱 cshcc@cshcc.cn 或拨打电话 010-88255986** 联系本机构技术信息部获取。

中标华信（北京）认证中心有限公司认证依据用标准或技术规范名称公开方式或可获取的途径：本中心按国家认监委要求备案及公示认证依据的封面和目录等关键信息，获取全文请购买和使用正版标准文件。

【认证规则、认证依据及认证证书公示信息及相关附件】

认证类别	认证领域	认证规则名称	认证规则编号	认证规则版本信息	状态标识	认证规则发布单位	认证规则发布/实施/修订日期	认证规则来源信息	认证依据用标准或技术规范名称	认证依据用标准或技术规范编号	认证依据用标准或技术规范发布单位	认证依据用标准或技术规范发布/实施日期	认证依据用标准或技术规范公开方式或可获取的途径	认证证书名称	认证证书与认证标志发布/所有权单位	认证证书样式	标志样式
管理体系	其他管理体系	公有云中保护个人可识别信息管理体系认证规则	CSHCC-RZGZ-PC-2025	A0	新建	中标华信（北京）认证中心有限公司	20260701	自行制定	信息技术-安全技术-作为 PII 处理者的公有云中保护个人可识别信息（PII）的操作规范	ISO/IEC 27018:2025	国际标准化组织；国际电工委员会	20250826	见附页	公有云中保护个人可识别信息管理体系认证证书	中标华信（北京）认证中心有限公司	见附页	不适用
									公有云中保护个人可识别信息管理体系认证技术规范	GB/T 22080-2025/ISO/IEC 27001:2022	国家市场监督管理总局；国家标准化管理委员会	20260101					

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-PC-2025 公有云中保护个人可识别信息管理体系认证规则及相关公示信息



公有云中保护个人可识别信息管理体系
认证规则

文件编号: CSHCC-RZGZ-PC-2025

文件版本: A0

编制：金鹏

复核：江雪

审核：伍倩惠

批准：刘伯钊

2026-06-02 首次发布

2026-07-01 实施

中标华信（北京）认证中心有限公司 发布

CSHCC-RZGZ-PC-2025

公有云中保护个人可识别信息管理体系认证规则

目录

1 适用范围	1
2 认证依据	4
3 对认证机构的基本要求	4
4 对认证人员的基本要求	5
5 认证程序	6
5.1 认证申请	6
5.2 申请评审	7
5.3 认证合同及相关责任	8
5.4 审核方案和审核策划	9
5.4.1 审核方案	9
5.4.2 审核时间	9
5.4.3 多场所抽样方案	10
5.4.4 组建审核组	10
5.4.5 审核计划	11
5.5 实施审核	11
5.6 初次认证审核	12
5.6.1 总则	12
5.6.2 第一阶段审核	12
5.6.3 第二阶段审核	13
5.7 监督审核	13
5.8 再认证审核	14
5.9 特殊审核	14
5.9.1 扩大认证范围	14
5.9.2 提前较短时间通知的审核	15
5.10 不符项及其验证	15

中标华信(北京)认证中心有限公司

2 / 27

CSHCC-RZGZ-PC-2025

公有云中保护个人可识别信息管理体系认证规则

5.11 审核报告.....	11
5.12 认证决定.....	16
6 认证证书和认证标志.....	17
6.1 总则.....	17
6.2 认证证书.....	18
6.3 认证标志.....	19
7 认证证书的暂停、撤销和注销.....	19
7.1 总则.....	19
7.2 认证证书的暂停.....	19
7.3 认证证书的撤销.....	20
7.4 认证证书的注销.....	20
8 申诉（投诉）处理.....	20
9 信息公开与报告.....	21
10 认证记录.....	21
11 其他.....	23
11.1 认证标准换届.....	23
11.2 内部审核.....	23
11.3 PCMS 技术服务.....	23
11.4 认证数据安全.....	23
12 附则.....	23
附录 A 公有云中保护个人可识别信息管理体系审核时间要求.....	25
附录 B 证书编号规则.....	26
修订记录.....	27

中标华信（北京）认证中心有限公司

3 / 27

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC-2025 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

	International Standard	ISO/IEC 27018:2025(en)
Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors <i>Sécurité de l'information, cybersécurité et protection de la vie privée — Lignes directrices en matière de protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII</i>	ISO/IEC 27018 Third edition 2025-08	 COPYRIGHT PROTECTED DOCUMENT
Reference number ISO/IEC 27018:2025(en)	© ISO/IEC 2025	© ISO/IEC 2025 All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester. ISO copyright office CP 401 • Ch. de Blandonnet 8 CH-1214 Vernier, Geneva Phone: +41 22 749 01 11 Email: copyright@iso.org Website: www.iso.org Published in Switzerland © ISO/IEC 2025 – All rights reserved ii

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-PC-2025 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

ISO/IEC 27018:2025(en)	
Contents	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview	3
4.1 Structure of this document	3
4.2 Control layout	10
5 Organizational controls	11
5.1 Policies for information security	11
5.2 Information security roles and responsibilities	11
5.3 Segregation of duties	11
5.4 Management responsibilities	11
5.5 Contact with authorities	11
5.6 Contact with special interest groups	12
5.7 Threat intelligence	12
5.8 Information security in project management	12
5.9 Inventory of information and other associated assets	12
5.10 Acceptable use of information and other associated assets	12
5.11 Return of assets	12
5.12 Classification of information	12
5.13 Labelling of information	12
5.14 Information transfer	12
5.15 Access control	12
5.16 Identity management	13
5.17 Authentication information	13
5.18 Access rights	13
5.19 Information security in supplier relationships	13
5.20 Addressing information security within supplier agreements	13
5.21 Managing information security in the ICT supply chain	13
5.22 Monitoring, review and change management of supplier services	13
5.23 Information security for use of cloud services	13
5.24 Information security incident management planning and preparation	13
5.25 Assessment and decision on information security events	13
5.26 Response to information security incidents	14
5.27 Learning from information security incidents	14
5.28 Collection of evidence	14
5.29 Information security during disruption	14
5.30 ICT readiness for business continuity	14
5.31 Legal, statutory, regulatory and contractual requirements	14
5.32 Intellectual property rights	14
5.33 Protection of records	14
5.34 Privacy and protection of PII	14
5.35 Independent review of information security	14
5.36 Compliance with policies, rules and standards for information security	15
5.37 Documented operating procedures	15
6 People controls	15
6.1 Screening	15
6.2 Terms and conditions of employment	15
6.3 Information security awareness, education and training	15
6.4 Disciplinary process	15
6.5 Responsibilities after termination or change of employment	15
6.6 Confidentiality or non-disclosure agreements	15

© ISO/IEC 2025 – All rights reserved
iii

ISO/IEC 27018:2025(en)	
6.7 Remote working	15
6.8 Information security event reporting	16
7 Physical controls	16
7.1 Physical security perimeters	16
7.2 Physical entry	16
7.3 Securing offices, rooms and facilities	16
7.4 Physical security monitoring	16
7.5 Protecting against physical and environmental threats	16
7.6 Working in secure areas	16
7.7 Clear desk and clear screen	16
7.8 Equipment siting and protection	16
7.9 Security of assets off-premises	16
7.10 Storage media	16
7.11 Supporting utilities	16
7.12 Cabling security	16
7.13 Equipment maintenance	17
7.14 Secure disposal or re-use of equipment	17
8 Technological controls	17
8.1 User endpoint devices	17
8.2 Privileged access rights	17
8.3 Information access restriction	17
8.4 Access to source code	17
8.5 Secure authentication	17
8.6 Capacity management	17
8.7 Protection against malware	17
8.8 Management of technical vulnerabilities	17
8.9 Configuration management	18
8.10 Information deletion	18
8.11 Data masking	18
8.12 Data leakage prevention	18
8.13 Information backup	18
8.14 Redundancy of information processing facilities	19
8.15 Logging	19
8.16 Monitoring activities	19
8.17 Clock synchronization	19
8.18 Use of privileged utility programs	19
8.19 Installation of software on operational systems	19
8.20 Networks security	19
8.21 Security of network services	19
8.22 Segregation of networks	20
8.23 Web filtering	20
8.24 Use of cryptography	20
8.25 Secure development lifecycle	20
8.26 Application security requirements	20
8.27 Secure system architecture and engineering principles	20
8.28 Secure coding	20
8.29 Security testing in development and acceptance	20
8.30 Outsourced development	20
8.31 Separation of development, test and production environments	20
8.32 Change management	21
8.33 Test information	21
8.34 Protection of information systems during audit testing	21
Annex A (informative) Public cloud PII processor extended control set for PII protection	22
Annex B (informative) Correspondence between this document and the first edition ISO/IEC 27018:2019	30
Bibliography	33

© ISO/IEC 2025 – All rights reserved
iv

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-PC-2025 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

 信息安全、网络安全和隐私保护—作为个人身份信息（PII）处理者的公共云中个人身份信息（PII）保护指南 信息安全、网络安全与隐私保护—关于在作为PII处理者的公共云中保护作为PII处理者的公共云中个人可识别信息（PII）的保护指南 参考编号 ISO/IEC 27018:2025(en)	国际标准 ISO/IEC 27018 2025 年 8 月 第 三版  受版权保护的文件 © ISO/IEC 2025 保留所有权利。除非另有说明，或在实施过程中有特殊要求，未经事先书面许可，不得以任何形式或任何手段（包括电子或机械方式，如复印、在互联网或内联网上发布）复制或其他方式使用本出版物的任何部分。许可申请可向下述地址的 ISO 或申请者所在国家的 ISO 成员机构提出。 ISO 版权办公室 CP 401 • Ch. de Blandornet 8 CH-1214 Vernier, 日内瓦, 电话: +41 22 749 01 11 电子邮件: copyright@iso.org 网站: www.iso.org 瑞士出版
--	--

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-PC-2025 公有云中保护个人可识别信息管理体系认证规则及相关公示信息

目录	页码
前言.....	v
引言.....	vi
1 范围.....	1
2 规范性引用.....	1
3 术语和定义.....	1
4 概述.....	3
4.1 本文件的结构.....	3
4.2 控制布局.....	10
5 组织控制.....	11
5.1 信息安全策略.....	11
5.2 信息安全角色和责任.....	11
5.3 职责分离.....	11
5.4 管理责任.....	11
5.5 与职能机构的联系.....	11
5.6 与特定相关方的联系.....	12
5.7 威胁情报.....	12
5.8 项目中的信息安全.....	12
5.9 信息及其他相关资产的清单.....	12
5.10 信息及其他相关资产的可接受使用.....	12
5.11 资产归还.....	12
5.12 信息分级.....	12
5.13 信息标记.....	12
5.14 信息传输.....	12
5.15 访问控制.....	12
5.16 身份管理.....	13
5.17 鉴别信息.....	13
5.18 访问权限.....	13
5.19 供应商关系中的信息安全.....	13
5.20 在供应商协议中强调信息安全.....	13
5.21 管理信息通信技术供应链中的信息安全.....	13
5.22 供应商服务的监视、评审和变更管理.....	13
5.23 云服务使用的信息安全.....	13
5.24 信息安全事件管理规划与准备.....	13
5.25 信息安全事件的评估与决策.....	13
5.26 信息安全事件的响应.....	14
5.27 从信息安全事件中学习.....	14
5.28 证据收集.....	14
5.29 中断期间的信息安全.....	14
5.30 业务连续性的信息通信技术就绪.....	14
5.31 法律、法规、规章和合同要求.....	14
5.32 知识产权.....	14
5.33 记录保护.....	14
5.34 隐私和个人可识别信息保护.....	14
5.35 信息安全的独立评审.....	14
5.36 符合信息安全的策略、规则 and 标准.....	15
5.37 文件化的操作规程.....	15
6 人员管控.....	15
6.1 审查.....	15
6.2 任用条款和条件.....	15
6.3 信息安全意识、教育和培训.....	15
6.4 违规处理过程.....	15
6.5 任用终止或变更后的责任.....	15
6.6 保密或不泄露协议.....	15

6.7 远程工作.....	15
6.8 信息安全事件的报告.....	16
7 物理控制.....	16
7.1 物理安全边界.....	16
7.2 物理入口.....	16
7.3 办公室、房间和设施的安全防护.....	16
7.4 物理安全监视.....	16
7.5 物理和环境威胁防范.....	16
7.6 在安全区域工作.....	16
7.7 清理桌面和屏幕.....	16
7.8 设备安置和保护.....	16
7.9 组织场所外的资产安全.....	16
7.10 存储媒体.....	16
7.11 支持性设施.....	16
7.12 布缆安全.....	16
7.13 设备维护.....	17
7.14 设备的安全处置或重复使用.....	17
8 技术控制措施.....	17
8.1 用户终端设备.....	17
8.2 特权访问权限.....	17
8.3 信息访问限制.....	17
8.4 源代码的访问.....	17
8.5 安全鉴别.....	17
8.6 容量管理.....	17
8.7 恶意软件防范.....	17
8.8 技术脆弱性管理.....	17
8.9 配置管理.....	18
8.10 信息删除.....	18
8.11 数据脱敏.....	18
8.12 数据防泄露.....	18
8.13 信息备份.....	18
8.14 信息处理设施的冗余.....	19
8.15 日志.....	19
8.16 监测活动.....	19
8.17 时钟同步.....	19
8.18 特权实用程序的使用.....	19
8.19 运行系统软件的安装.....	19
8.20 网络安全.....	19
8.21 网络服务的安全.....	19
8.22 网络隔离.....	20
8.23 网页过滤.....	20
8.24 密码技术的使用.....	20
8.25 安全开发生存周期.....	20
8.26 应用程序安全要求.....	20
8.27 系统安全架构和工程原则.....	20
8.28 安全编码.....	20
8.29 开发和验收中的安全测试.....	20
8.30 开发外包.....	20
8.31 开发、测试和生产环境的隔离.....	20
8.32 变更管理.....	21
8.33 测试信息.....	21
8.34 在审计测试中保护信息系统.....	21
附件 A（参考性）公共云个人信息（PII）处理器扩展控制集（用于 PII 保护）.....	22
附录 B（参考性）本文件与 ISO/IEC 27018:2019 第一版之间的对应关系.....	30
参考文献.....	33

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则
CSHCC-RZGZ-PC-2025 公有云中保护个人可识别信息管理体系认证规则及相关公示信息



中标华信(北京)认证中心
CSHCC.CN

公有云中保护个人可识别信息
管理体系认证证书

证书编号: XXXXXXXXXXXXX

兹证明
XXXXXXXXXXXX 有限公司

统一社会信用代码: XXXXXXXXXXXXXXXX
注册地址: XXXXXXXXXXXXXXXXXXXX
办公地址: XXXXXXXXXXXXXXXXXXXX
生产地址: XXXXXXXXXXXXXXXXXXXX

公有云中保护个人可识别信息管理体系符合标准:
GB/T 22080-2025/ISO/IEC 27001:2022
《网络安全技术 信息安全管理要求》
ISO/IEC 27018:2025《信息安全、网络安全和隐私保护—作为个人信息
信息 (PII) 处理者的公共云中个人信息 (PII) 保护指南》

通过认证的范围:
与 XXXX 相关的在公有云中保护个人信息的信息安全管理活动
(适用性声明版本: XXXX)

本证书在国家规定的各行政许可、资质许可有效期内使用有效,
在接受监督审核并经审核合格后,与证书下方二维码一并使用有效。

发证日期: XXXX-XX-XX 初次发证: XXXX-XX-XX
有效期至: XXXX-XX-XX 换证日期: XXXX-XX-XX

签发: 刘例刘 中标华信(北京)认证中心
有限公司



中心地址: 北京市石景山区石景山路3号玉泉大厦5层 中心电话: 010-88255986 中心邮编: 100049
注: 证书详细信息可在国家认证认可监督管理委员会官方网站 (www.cnca.gov.cn)
及本机构网站 (www.cshcc.cn) 或扫描左侧二维码查询



中标华信(北京)认证中心
CSHCC.CN

Authentication Certificate of Protection of
PII in Public Clouds Management Systems

Registration No. XXXXXXXXXXXXXXXX

This is to certify that
XXXXXXXXXXXX Ltd.

Unified Social Credit Code: XXXXXXXXXXXXXXXX
Registered Address: XXXXXXXXXXXXXXXXXXXX
Office Address: XXXXXXXXXXXXXXXXXXXX
Production Address: XXXXXXXXXXXXXXXXXXXX

Protection of PII in Public Clouds Management Systems satisfy:
GB/T 22080-2025/ISO/IEC 27001:2022 Cybersecurity technology—
Information security management systems—Requirements
ISO/IEC 27018:2025 Information security, cybersecurity and privacy protection—
Privacy information management systems—Requirements and guidance

The certificate is valid for the following scope:
Information security management activities related to XXXX
to protect personal identity information in public clouds
(Statement of Applicability: XXXX)

This certificate is valid for use within the validity period of various administrative and
qualification licenses stipulated by the state. It is valid when used together with the QR code below the certificate
after undergoing supervision audit and passing the review.

Date of Issue: XXXX-XX-XX Date of Initial Certification: XXXX-XX-XX
Date of Expiry: XXXX-XX-XX Date of Change: XXXX-XX-XX

Profound Lin
General Manager

China Standard Huaxin (Beijing)
Certification Center Co., Ltd.



Address of Certification Authority: 5 Floor, YuQuan Building No.3 Shijingshan Road, Shijingshan District, Beijing Tel: 010-88255986 P.C.: 100049
Note: The detailed information is available on the Certification and Accreditation Administration of the People's Republic of China official website
(www.cnca.gov.cn) the authority's website (www.cshcc.cn) and the Quick Response Code on the left.